National Security Agency/Central Support Service

INFORMATION
ASSURANCE
DIRECTORATE

CGS Vulnerability Assessment Capability

Version 1.1.1

Vulnerability Assessment is the systematic examination of an Enterprise to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

07/30/2012

CGS Vulnerability Assessment Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

A vulnerability is a weakness that has the potential to reduce an Enterprise's ability to fulfill its mission. Vulnerability Assessment is the systematic examination of an Enterprise to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. Vulnerability alerts are released to initiate follow-on functions.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of "good enough" when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

Vulnerabilities are a serious concern for every Enterprise. Proper assessment of vulnerabilities is essential to maintaining operational security by providing mechanisms that are automated, where possible, for identifying and examining vulnerabilities caused by software flaws, system misconfigurations, physical deterioration, and process flaws, as well as physical and personnel security concerns.

The Vulnerability Assessment Capability shall identify information technology vulnerabilities by accessing automated, up-to-date sources of vulnerability information that provide output that is machine consumable (e.g., in a form that can be directly fed into a database), such as the National Vulnerability Database (NVD), as opposed to information provided using manual methods such as email distribution. Once in the database, the information shall be automatically assessed for applicability based on alignment with the Enterprise asset information. There shall be a validation mechanism that ensures the applicability is assigned correctly. Information shall then be automatically prioritized for review based on device mission, potential impact, and location on a network (e.g., operational versus nonoperational, behind a firewall versus wider exposure, test lab). Scoring and reporting mechanisms provided by the Vulnerability Assessment

Capability shall be provided in a standard format, such as the eXtensible Markup Language (XML) format used by the NVD. When follow-on analysis is warranted, vulnerability alerts shall be composed, reviewed prior to release to minimize false positives, and then sent to other Community Gold Standard Capabilities for disposition.

In addition to looking at already published vulnerabilities, the Vulnerability Assessment Capability includes considerations for identifying unique or unpublished vulnerabilities. Often it is not a single weakness in isolation that creates a vulnerability but rather a set of weaknesses in one or several interconnected systems that together create a vulnerability. The Enterprise needs to be able to scan for and identify unique vulnerabilities such as these.

Identified potential vulnerabilities shall be sent to other Capabilities (see Capability Interrelationships section), resulting in further analysis and information received from those Capabilities, which shall contribute to overall situational awareness. The database of active vulnerabilities under review shall have a search function or the ability to run ad hoc queries to assess status and trends. Vulnerability status information shall be reported in accordance with established Enterprise requirements as well as be discoverable and accessible to peer Organizations and others, as appropriate.

Physical, environmental, and personnel security vulnerabilities exist and represent a significant concern. These vulnerabilities are likewise addressed by other Capabilities that benefit from Vulnerability Assessment but are not typically managed within the same asset system that manages information technology vulnerabilities. Technical surveillance and countermeasures and counter-intelligence are established Enterprise programs that also identify and share information related to these types of vulnerabilities. Similarly, acquisition activities manage related vulnerabilities (e.g., operations security, supply chain) within the Enterprise. These programs shall be tightly coupled with the asset database to link the systems and process that affect Enterprise-wide vulnerabilities.

The Vulnerability Assessment capability shall also use a defined set of security protections (or controls) that are applicable to the Enterprise to determine whether vulnerabilities exist within the Enterprise. Assessment against these protections shall provide insight to any security gaps, thus identifying a potential vulnerability and shall provide information on the depth and breadth of exposure of a particular vulnerability. The required protection or security control information shall be provided by multiple capabilities across the Community Gold Standard and is also directed by policy (see

Security Control Tables for all Community Gold Standard Capabilities and the Policy and Directives Table below).

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Enterprise systems are complex enough that vulnerabilities should be expected.
2. The mission is understood.
3. Configuration management knows which systems have been patched or configured to mitigate a known vulnerability.
4. Automated, up-to-date sources of vulnerability information are available that provide output that is machine consumable (e.g., in a form that can directly fed into a database)
5. There will always be some vulnerability information that is available only in non-automated form.
6. System inventory information (hardware and software asset database) is available to enable assessment of potential applicability of vulnerabilities based on the components that compose the system.
7. System component location and information pertaining to mission criticality are available to inform the prioritization of vulnerabilities.
8. Technical surveillance and countermeasures and counter-intelligence services are available and provide assessment of physical and environmental security and personnel security vulnerabilities.
9. A set of required security controls or protections is available to the Organization to identify and assess exposure of vulnerabilities.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability initiates various analysis and remediation activities.
2. The Capability provides a reporting mechanism for known vulnerabilities affecting each personnel, operational, technical, or environmental component.
3. The Capability has research personnel available to monitor and identify new sources of vulnerability information for incorporation.

4. The Capability is able to accommodate vulnerability information also available only in non-automated form.
5. The Capability is able to import data from other Capabilities that are needed to identify vulnerabilities, make an applicability determination, prioritize potential vulnerabilities, support situational awareness, and measure effectiveness.
6. The Capability incorporates a human review prior to releasing vulnerability alerts to other Capabilities to minimize false positives.
7. The Capability provides mechanisms to determine the severity of the vulnerability based on network context.
8. The Capability provides vulnerability identification and assessment information that may be used by compliance or accreditation activities.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When Vulnerability Assessment is implemented correctly, the Organization will possess a capability to effectively assess its known vulnerabilities. Vulnerabilities can exist in both the physical world and in information technology systems. Physical vulnerabilities cover any means by which an attacker could gain unauthorized physical access to secure facilities or information and also any environmental factors that could lead to a disruption of mission operations. Information technology vulnerabilities can be the result of such things as software flaws, system misconfigurations, or physical deterioration.

Regarding information technology, the Capability will identify and obtain information about potential vulnerabilities, assess applicability of those potential vulnerabilities to the system, prioritize candidate vulnerabilities, and initiate vulnerability alerts. Appropriate security measures will be in place to enable access to sources of machine-consumable vulnerability information across differing security domains. The content and formats of information from such sources will ideally conform to common formats (e.g., Common Vulnerabilities and Exposures [CVE], Common Platform Enumeration [CPE™], and Common Configuration Enumeration [CCE™]) to enable cross-platform interoperability.

Vulnerability information for some assets may not be reportable via near real-time feeds, so these sources will be checked no less frequently than monthly. Research personnel will be available to monitor and identify new sources of vulnerability information for incorporation into the Capability. Ratings provided by information sources will contribute to applicability and severity determinations. Critical vulnerability information that is available only in non-automated form will be accommodated. Potential vulnerability information can also come from other Capabilities (e.g., Security Assessments and Enterprise Audit Assessment), which communicate using standardized formats and protocols.

Applicability assessment and prioritization will be possible because the Capability will seamlessly communicate with other Capabilities that provide system inventory information, component location, and mission requirements. The results will be vulnerability alerts that are submitted to other Capabilities for further processing.

As other Capabilities perform their respective tasks, feedback will be communicated to Vulnerability Assessment for consolidation, trend analysis, status display, and reporting in support of decision-maker situational awareness. This can include feedback from Vulnerability Assessment Capabilities that exist in other processes or systems, which departments or agencies have in place to address physical and environmental security and personnel security vulnerabilities.

Not all vulnerabilities need to be altogether eliminated. Such a goal would be unrealistic and prohibitively expensive. All vulnerabilities have an associated level of risk that they will be exploited and an estimated cost if such an exploit were to occur. All vulnerabilities shall be eliminated where it is operationally efficient to do so, that is, if the total expected cost of a given vulnerability getting exploited (possibly many times) exceeds the total cost to eliminate that vulnerability, the Organization will take the steps necessary to eliminate that vulnerability. Any vulnerabilities that cannot be eliminated should be assessed and, if possible, appropriate steps should be taken to mitigate the risk that the vulnerabilities produce.

Organizations will monitor for vulnerabilities using resources such as:

- Enterprise patch assessment tools, to obtain all available patches from supported vendors.
- Vendor security mailing lists and websites, to obtain all available patches from vendors not supported by the Enterprise patch assessment tool.
- Vulnerability database or mailing list to obtain immediate information on all known vulnerabilities and suggested remediations (e.g., the NVD).

- Third-party vulnerability mailing lists that highlight the most critical vulnerabilities (e.g., the US Computer Emergency Readiness Team [US-CERT] Cyber Security Alerts). Such lists will help Organizations focus on the most important vulnerabilities that may be overlooked among myriad vulnerabilities published by more general vulnerability resources.
- Inspections of protections or security control sets to determine whether controls or protections that are required are not in place.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping–The Vulnerability Assessment Capability relies on information from the Network Mapping Capability to align a vulnerability to the Enterprise assets, make a preliminary assessment of a vulnerability's applicability to the system, prioritize alerts, and measure effectiveness.
- Network Boundary and Interfaces–The Vulnerability Assessment Capability relies on information from the Network Boundary and Interfaces Capability to align a vulnerability to the Enterprise assets, make a preliminary assessment of a vulnerability's applicability to the system, prioritize alerts, and measure effectiveness.
- Utilization and Performance Management–The Vulnerability Assessment Capability relies on information from the Utilization and Performance Management Capability to align a vulnerability to the Enterprise assets, make a preliminary assessment of a vulnerability's applicability to the system, prioritize alerts, and measure effectiveness.
- Understand Mission Flows–The Vulnerability Assessment Capability relies on information from the Understand Mission Flows Capability to align a vulnerability to the Enterprise assets, make a preliminary assessment of a vulnerability's applicability to the system, prioritize alerts, and measure effectiveness.

- Understand Data Flows–The Vulnerability Assessment Capability relies on information from the Understand Data Flows Capability to align a vulnerability to the Enterprise assets, make a preliminary assessment of a vulnerability's applicability to the system, prioritize alerts, and measure effectiveness.
- Hardware Device Inventory–The Vulnerability Assessment Capability relies on information from the Hardware Device Inventory Capability to align a vulnerability to the Enterprise assets, make a preliminary assessment of a vulnerability's applicability to the system, prioritize alerts, and measure effectiveness.
- Software Inventory–The Vulnerability Assessment Capability relies on information from the Software Inventory Capability to align a vulnerability to the Enterprise assets, make a preliminary assessment of a vulnerability's applicability to the system, prioritize alerts, and measure effectiveness.
- Understand the Physical Environment–The Vulnerability Assessment Capability relies on information from the Understand the Physical Environment Capability to align a vulnerability to the Enterprise assets, make a preliminary assessment of a vulnerability's applicability to the system, prioritize alerts, and measure effectiveness.
- Configuration Management–The Vulnerability Assessment Capability relies on the Configuration Management Capability to provide information that contributes to determining applicability of a vulnerability.
- Incident Analysis–The Vulnerability Assessment Capability relies on the Incident Analysis Capability to feed information about the root cause of an incident such that a decision can be made about whether the incident presents a vulnerability for the Enterprise. The Vulnerability Assessment Capability also relies on the Incident Analysis Capability to provide information that is used to measure the effectiveness of its assessment decisions.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Vulnerability Assessment Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Vulnerability Assessment Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.

- IA Awareness–The Vulnerability Assessment Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Vulnerability Assessment Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Organizations and Authorities Capability establishes the roles and responsibilities assigned to the Vulnerability Assessment Capability.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Network Security Evaluations–The Vulnerability Assessment Capability relies on the Network Security Evaluations Capability to provide information that may be used in the scoping of evaluation activities.
- Network Hunting–The Vulnerability Assessment Capability relies on the Network Hunting Capability to provide information to support the detection of vulnerabilities.
- Physical Hunting–The Vulnerability Assessment Capability relies on the Physical Hunting Capability to provide information to support the detection of vulnerabilities.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	**Related Text**
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
AT-5 *CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS*	Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community: - To facilitate ongoing security education and training for organizational personnel; - To stay up to date with the latest recommended security practices, techniques, and technologies; and

	- To share current security-related information including threats, vulnerabilities, and incidents. Enhancement/s: None Specified
CA-7 *CONTINUOUS MONITORING*	Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials [Assignment: organization-defined frequency]. Enhancement/s: (1) The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.
RA-5 *VULNERABILITY SCANNING*	Control: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability assessment process by using standards for: Enumerating platforms, software flaws, and improper configurations; Formatting and making transparent, checklists and test procedures; and Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated

	personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). Enhancement/s: (1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. (2) The organization updates the list of information system vulnerabilities scanned [Assignment: organization-defined frequency] or when new vulnerabilities are identified and reported. (3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked). (4) The organization attempts to discern what information about the information system is discoverable by adversaries. (5) The organization includes privileged access authorization to [Assignment: organization-identified information system components] for selected vulnerability scanning activities to facilitate more thorough scanning. (6) The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities. (7) The organization employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials. (8) The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited. (9) The organization employs an independent penetration agent or penetration team to: (a) Conduct a vulnerability analysis on the information system; and (b) Perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.

SI-5 *SECUTITY ALERTS, ADVISORIES, AND DIRECTIVES*	Control: The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to [Assignment: organization-defined list of personnel (identified by name and/or by role)]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. Enhancement/s: (1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.
SI-6 *SECURITY FUNCTIONALITY VERIFICATION*	Control: The information system verifies the correct operation of security functions [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered. Enhancement/s: (1) The information system provides notification of failed automated security tests. (2) The information system provides automated support for the assessment of distributed security testing. (3) The organization reports the result of security function verification to designated organizational officials with information security responsibilities.
SI-7 *SOFTWARE AND INFORMATION INTEGRITY*	Control: The information system detects unauthorized changes to software and information. Enhancement/s: (1) The organization reassesses the integrity of software and information by performing [Assignment: organization-defined frequency] integrity scans of the information system.

	(2) The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification. (3) The organization employs centrally managed integrity verification tools. (4) The organization requires use of tamper-evident packaging for [Assignment: organization-defined information system components] during [Selection: transportation from vendor to operational site; during operation; both].

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Vulnerability Assessment Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 503 IC Information Technology Systems Security Risk Management, Certification and Accreditation, 15 September 2008, Unclassified	Summary: This directive addresses risk assessment and certification. Vulnerability identification and assessment is part of these activities.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDD 8100.02 Use of Commercial Wireless	Summary: This directive addresses vulnerability and vulnerability mitigation, which is interpreted to be

Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 23 April 2007, Unclassified	Vulnerability Assessment. Purpose 1.2. Directs the development and use of a Knowledge Management (KM) process to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the Department of Defense. Policy 4.10. A DoD wireless KM process shall be established. The goal is increased sharing of DoD wireless expertise to include information on vulnerability assessments, best practices, and procedures for wireless device configurations and connections.
DoDI 8110.1 Multinational Information Sharing Networks Implementation, 6 February 2004, Unclassified	Summary: This instruction addresses multinational information sharing networks. "Paragraph 5.8.5, Provide for the type-security test and certification of MNIS CENTRIXS networks, their interfaces to each other, and their interfaces to U.S. networks, as appropriate, in accordance with reference (e), or its revisions, including primary responsibility for defining, validating, and promulgated security test and evaluation standards. The MNISPMO retains primary responsibility for acknowledging, managing, coordinating, and disseminating IAVA alerts, establishing corrective action plan, and reporting overall compliance to the JTF-CNO as a participant in the Vulnerability Assessment System (VMS)…"
DoDD 8500.01E Information Assurance (IA), 23 April 2007, Unclassified	Summary: This directive sets policy related to Vulnerability Assessment: Policy: 4.21. Identified DoD information system vulnerabilities shall be evaluated for DoD impact, and tracked and mitigated…
DoD I 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007, Unclassified	Summary: This instruction addresses certification and accreditation. It includes: 5. Responsibilities: 5.16. The Program Manager (PM) or System Manager (SM) for DoD ISs shall: 5.16.3. Plan and budget for IA controls implementation, validation, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability assessment.
DoD 8580.02-R DoD	Summary: This regulation addresses information security

Health Information Security Regulation, 12 July 2007, Unclassified	responsibilities for health information technology (IT) systems. C1.6.3. The Heads of the DoD Components shall: C1.6.3.4. Provide for vulnerability mitigation and an incident response and reporting capability that encompasses electronic PHI.
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified	This Joint Staff Instruction assigns Vulnerability Assessment responsibilities to various Department of Defense (DoD) Organizations.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Vulnerability Assessment Standards

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	

Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
NIST SP 800-30 Risk Assessment Guide for Information Technology Systems, July 2002, Unclassified	Summary: This special publication (SP) addresses Risk Assessment. "Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization." Actual vulnerabilities must be identified to pass on to the risk assessment process.
NIST SP 800-40 Ver. 2 Creating a Patch and Vulnerability Assessment Program, November 2005, Unclassified	Summary: This SP addresses Vulnerability Assessment. Patch and Vulnerability Assessment is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an Organization.
NIST SP 800-70 Rev 1 National Checklist Program for IT Products–Guidelines for Checklist Users and Developers, Sept 2009, Unclassified	Summary: "… The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products. …" Checklists can be a tool in the Vulnerability Assessment process.
NIST SP 800-117, Guide to Adopting and Using the Security Content Automation Protocol (SCAP), July 2010, Unclassified	Summary: This SP provides a conceptual level overview of the Security Content Automation Protocol (SCAP). SCAP comprises a suite of specifications for organizing and expressing security-related information in standardized ways, as well as related reference data, such as identifiers for software flaws and security configuration issues. It can be used for maintaining the security of Enterprise systems, such as automatically verifying the installation of patches, checking system security configuration settings, and examining systems for signs of compromise. A SCAP-expressed checklist documents desired security configuration settings, installed patches, and other system security elements in a standardized format.
NIST SP 800-126, The Technical Specification for the Security Content Automation Protocol,	Summary: This SP provides the definitive technical specification for Version 1.0 of the SCAP, consisting of a suite of specifications for standardizing the format and nomenclature by which security software communicates

November 2009, Unclassified	information about software flaws and security configurations. [See entry above for SP 800-117]
NIST National Vulnerability Database (NVD) Version 2.2, Unclassified	The National Vulnerability Database (NVD) is the U.S. government repository of standards-based Vulnerability Assessment data represented using the SCAP. This data enables automation of Vulnerability Assessment, security measurement, and compliance. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Common Configuration Enumeration (CCE™) MITRE manages and maintains the creation of the CCE List with assistance from the CCE Working Group, conducts community outreach activities, maintains the CCE public website, and provides neutral guidance throughout the process to ensure that CCE serves the public interest. http://cce.mitre.org, Unclassified	Summary: Common Configuration Enumeration (CCE™) provides unique identifiers to security-related system configuration issues to improve workflow by facilitating fast and accurate correlation of configuration data across multiple information sources and tools. CCE identifiers can be used to associate checks in configuration assessment tools with statements in configuration best practice. CCE identifiers are the main identifiers used for the settings in the U.S. Federal Desktop Core Configuration (FDCC) data file downloads; and provide a mapping between the elements in configuration best practice documents including National Institute of Standards and Technology's (NIST) Security Configuration Guides, National Security Agency's (NSA) Security Configuration Guides, and Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGS). CCE is also one of six existing open standards used by NIST in its SCAP program, which combines "a suite of tools to help automate vulnerability assessment and evaluate compliance with federal information technology security requirements." Numerous products have been validated by NIST as

	conforming to the CCE component of SCAP.
Common Platform Enumeration (CPE™) http://cpe.mitre.org, Unclassified	Summary: Common Platform Enumeration (CPE™) is a structured naming scheme for IT systems, platforms, and packages. Based on the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name. CPE provides a more formal, consistent, and uniform naming scheme that allows tools (as well as humans) to clearly identify the IT platforms to which a vulnerability or element of guidance applies. The CPE Specification includes a naming syntax and conventions for constructing CPE names from product information, an algorithm for matching, a language for describing complex platforms, and an eXtensible Markup Language (XML) schema for binding descriptive and diagnostic information to a name.
Common Vulnerabilities and Exposures (CVETM). MITRE maintains CVE, manages the compatibility program, maintains the CVE public website, and provides impartial technical guidance to the CVE Editorial Board throughout the process to ensure that CVE serves the public interest. http://cve.mitre.org, Unclassified	Summary: Common Vulnerabilities and Exposures (CVE) is a dictionary of common names (i.e., CVE Identifiers) for publically known information security vulnerabilities and exposures. CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an Organization's security tools. The report from a security tool that incorporates CVE identifiers enables information to be quickly and accurately accessed from one or more separate CVE compatible databases to remediate the problem. CVE's use is widespread in many areas including vulnerability management, vulnerability alerting, patch management, and intrusion detection.

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Uploads from public sources–Added security is necessary to enable data uploads from public sources to the Top Secret (TS) environment.
2. Manpower to implement, maintain, and execute–The Enterprise will need to have or obtain the necessary personnel to understand purchasing, implementation, and execution.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Vulnerability Assessment Capability.

- The Enterprise shall perform systematic examinations to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation to ensure that an Enterprise can fulfill its mission.
- The Enterprise shall identify information technology vulnerabilities by accessing automated, up-to-date sources of vulnerability information that provide output that is machine consumable (e.g., in a form that can be directly fed into a database), such as the NVD, as opposed to information provided using manual methods such as email distribution.
- The Enterprise shall include considerations for identifying unique or unpublished information security vulnerabilities.

- Vulnerability information shall be automatically assessed for applicability based on alignment with the Enterprise asset information. There shall be a validation mechanism that ensures the applicability is assigned correctly.
- Vulnerability information shall be automatically prioritized for review based on device mission, potential impact, and location on a network (e.g., operational versus nonoperational, behind a firewall versus wider exposure, test lab).
- Information technology vulnerabilities identified by the Enterprise shall be tightly coupled with physical, environmental, personnel security, operations security, and supply chain vulnerabilities to link the systems and process that affect Enterprise-wide vulnerabilities.
- The Enterprise shall use a defined set of security protections (or controls) that are applicable to the Enterprise. Assessment against these protections shall provide insight into any security gaps, thus identifying a potential vulnerability and shall provide information on the depth and breadth of exposure of a particular vulnerability.
- When follow-on analysis is warranted, vulnerability alerts shall be composed, reviewed prior to release to minimize false positives, and provided for disposition.
- Scoring and reporting mechanisms provided by the Enterprise shall be provided in a standard format, such as the XML format used by the NVD.
- Identified potential vulnerabilities shall be sent for further analysis to contribute to overall situational awareness.
- The database of active vulnerabilities under review shall have a search function or the ability to run ad hoc queries to assess status and trends.
- Vulnerability status information shall be reported in accordance with established Enterprise requirements as well as be discoverable and accessible to peer Organizations and others, as appropriate.